UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/783,122	02/19/2004	Michael B. Shelby	IGT1P306X1/AC022 CIP	1230

79646 7590 06/18/2009

Weaver Austin Villeneuve & Sampson LLP - IGT
Attn: IGT
P.O. Box 70250
Oakland, CA 94612-0250

EXAMINER	
DUFFY, DAVID W	

ART UNIT	PAPER NUMBER
3714	

MAIL DATE	DELIVERY MODE
06/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/783,122	SHELBY ET AL.	
	Examiner	Art Unit	
	DAVID DUFFY	3714	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04/17/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. This office action is in response to the amendment filed 04/17/2009 in which applicant amends claims 1, 9, 16 and 21. Claims 1-23 are pending.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 04/17/2009 has been entered.

Information Disclosure Statement

3. The information disclosure statement filed 04/17/2009 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered unless otherwise indicated.

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1-4, 8, and 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen, Binh T. US 20020071557 A1 in view of Federal Information Processing Standards Publication 186 (FIPS) and Staring, Antonius A.M. (US 20010007127 A1).

6. In regard to claim 1, Nguyen discloses generating a command at a master server or slave server, digitally signing it and transmitting to a receiving node for re-hashing and verification (fig 4, elements 400-420). Nguyen does not explicitly disclose digitally signing the command by performing a hashing function over at least a portion of a message that includes the command to produce a message digest and passing the message digest through a digital signature algorithm to produce a digitally signed command; verification wherein the digitally signed command from the transmitting mode is subjected to the hashing function to produce a message digest, the message digest is passed through the digital signature algorithm to produce a digitally signed command at the receiving node, and the digitally signed command at the receiving node is compared to the digitally signed command from the transmitting mode to determine if there is a match.

7. In related prior art, FIPS discloses a digital signature standard that digitally signs a message by using a hash function in the signature generation process to obtain a condensed version of data, called a message digest (see Figure 1). The message digest is then input to the DSA to generate the digital signature. The digital signature is sent to the intended verifier along with the signed data (often called the message). The verifier of the message and signature verifies the signature by using the sender's public

key. The same hash function must also be used in the verification process. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data. One skilled in the art would recognize the advantages of providing a secure way to authenticate the sender of a message in a network environment.

8. Therefore it would have been obvious to one skilled in the art at the time of the invention to have modified Nguyen in view of FIPS in order to have included the digital signature method of FIPS in order to provide a secure authentication process. The combination made lacks including a session key that is changeable and associated with an index so that a receiving node can determine the session key used.

9. In related prior art, Staring discloses that in encrypted systems it is useful to change session keys periodically (par 2) where the session keys are indexed so that a receiving node can determine the session key used (pars 12-14) to facilitate session key changes without the requirement of knowing what the decrypted data should look like (par 5). Staring further discloses that each message includes a session index portion that is used to determine the session index of the receiving device in order to properly decrypt the message by testing the current and future session keys (par 40). Under this procedure, each message sent from the source includes the updated session key and each receiver knows the current session key that they are using. The receiving node thus is able to determine from the message what the updated session index and the corresponding key is from the key check data. One of ordinary skill in the art would recognize the advantages of changing session keys in order to increase security and

providing a way for the receiving nodes to ensure they are using the proper key for decryption.

10. Therefore it would have been obvious to one of ordinary skill in the art to have modified Nguyen in view of Staring to have incorporated a session key index to facilitate frequent key changes for enhanced security while providing a way for the devices to determine the current session key to use. The combination does not explicitly disclose that the receiving node requests a new session key when the session index does not match the updated index.

11. However, one of ordinary skill in the art would have recognized that when applying the session index key check of Staring to a system where the receiving nodes did not have the ability to generate keys, it would be necessary for the clients to request a new key when the key check taught by Staring failed to match since such a system would have no more keys to try. Such a modification would have been readily understood by one of ordinary skill in the art, would have produced the expected result of getting the proper key to the device as would be needed to ensure operation of the system, and would be in keeping with the teachings of Staring to implement. Accordingly, such a modification does not differentiate over the prior art.

12. In regard to claim 2, Nguyen discloses that the gaming machine generates encrypted data messages based on machine transactions (fig 4, elements 400-406). Examiner contends that this constitutes monitoring events to generate a command.

13. In regard to claim 3, Nguyen discloses that the remote server or master of the system receives messages from the gaming machine and responds to the message (fig

4, elements 426-431). Examiner contents that this constitutes monitoring events on the gaming machine by the master server as it receives event information from the gaming machine thereby monitoring the event. Nguyen further discloses that the local server or slave receives the signed command (fig 4, element 408).

14. In regard to claim 4, Nguyen discloses that the slave server processes and stores data generated by the gaming machine before re-encrypting and sending it to the master server (fig 4, element 412). Examiner contends that by storing the data the slave server is inherently monitoring the activities of the gaming machine. Nguyen further discloses sending a command from the master server to the gaming machine that the gaming machine verifies (fig 6).

15. In regard to claim 8, Nguyen discloses that encryption may be optional over a dedicated communication network and then applied when the message reaches an unsecured channel (11:39-47)

16. In regard to claims 16 and 17, Nguyen discloses the receiving of commands with digital signatures and verifying the signatures at a slave device (par 58). Nguyen lacks explicitly stating verifying the digital signature at the subservient device by subjecting the command message to a hashing function to produce a message digest, passing the message digest through a digital signature algorithm to produce a digital signature at the subservient device, and comparing the digital signature at the subservient device to the digital signature included with the command message to determine if there is a match; and executing the command message at the subservient device, if the signatures verify.

17. In related prior art, FIPS discloses a digital signature standard that digitally signs a message by using a hash function in the signature generation process to obtain a condensed version of data, called a message digest (see Figure 1). The message digest is then input to the DSA to generate the digital signature. The digital signature is sent to the intended verifier along with the signed data (often called the message). The verifier of the message and signature verifies the signature by using the sender's public key. The same hash function must also be used in the verification process. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data. One skilled in the art would recognize the advantages of providing a secure way to authenticate the sender of a message in a network environment.

18. Therefore it would have been obvious to one skilled in the art at the time of the invention to have modified Nguyen in view of FIPS in order to have included the digital signature method of FIPS in order to provide a secure authentication process. The combination made lacks including a session key that is changeable and associated with an index so that a receiving node can determine the session key used.

19. In related prior art, Staring discloses that in encrypted systems it is useful to change session keys periodically (par 2) where the session keys are indexed so that a receiving node can determine the session key used (pars 12-14) to facilitate session key changes without the requirement of knowing what the decrypted data should look like (par 5). Staring further discloses that each message includes a session index portion that is used to determine the session index of the receiving device in order to properly decrypt the message by testing the current and future session keys (par 40).

Under this procedure, each message sent from the source includes the updated session key and each receiver knows the current session key that they are using. The receiving node thus is able to determine from the message what the updated session index and the corresponding key is from the key check data. One of ordinary skill in the art would recognize the advantages of changing session keys in order to increase security and providing a way for the receiving nodes to ensure they are using the proper key for decryption.

20. Therefore it would have been obvious to one of ordinary skill in the art to have modified Nguyen in view of Staring to have incorporated a session key index to facilitate frequent key changes for enhanced security while providing a way for the devices to determine the current session key to use. The combination does not explicitly disclose that the receiving node requests a new session key when the session index does not match the updated index.

21. However, one of ordinary skill in the art would have recognized that when applying the session index key check of Staring to a system where the receiving nodes did not have the ability to generate keys, it would be necessary for the clients to request a new key when the key check taught by Staring failed to match since such a system would have no more keys to try. Such a modification would have been readily understood by one of ordinary skill in the art, would have produced the expected result of getting the proper key to the device as would be needed to ensure operation of the system, and would be in keeping with the teachings of Staring to implement. Accordingly, such a modification does not differentiate over the prior art.

22. In regard to claim 18, Nguyen discloses that the gaming device may receive signed messages and validate them (par 73).

23. In regard to claim 19, Nguyen discloses generating a signed command at the master server, sending it to the slave server, and the slave server decrypting the message and forwarding to the gaming machine (par 62).

24. Claims 5-7 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen, Binh T. (US 20020071557 A1) in view of Federal Information Processing Standards Publication 186 (FIPS) and Staring, Antonius A.M. (US 20010007127 A1) as applied to claims 1 and 16 above, and further in view of Torango et al. (USPN 5885158).

25. In regard to claims 5 and 6, Nguyen in view of FIPS and Staring discloses the method of claim 1 above, but lacks wherein the event further comprises an event triggering a bonus is to be paid or wherein the command further comprises a bonus command.

26. In related prior art, Torango discloses a bonus system that generates bonus commands based on bonus triggering events (15:41-51). One skilled in the art would recognize the advantages of providing a progressive bonus game on a networked system in order to attract more players to a casino through higher potential payouts.

27. Therefore it would have been obvious to one skilled in the art at the time to combine the secure system of Nguyen in view of FIPS and Staring with the progressive system of Torango to provide a secure progressive system that would attract customers by offering larger potential payouts via a large group of networked devices.

28. In regard to claim 7, Nguyen discloses generating a signed command at the master server, sending it to the slave server, and the slave server decrypting the message and forwarding to the gaming machine (par 62). Nguyen lacks explicitly stating that the message is a bonus command.

29. In related prior art, Torango discloses a bonus system that generates bonus commands (15:41-51). One skilled in the art would recognize the advantages of providing progressive games on a networked system to increase the size of the contributing player pool thereby offering larger potential payouts in order to attract players.

30. Therefore it would have been obvious to one skilled in the art at the time to combine the secure system of Nguyen with the progressive system of Torango to provide a secure progressive system thus providing large potential payouts to attract customers. Nguyen in view of Torango lacks explicitly stating that the reply message is re-signed before sending it to the gaming machine.

31. However, Nguyen already discloses signing the messages on the way to the slave server from the gaming device (fig 4) and discloses that the slave server decrypts and then forwards the message to the gaming machine as stated above. It would be obvious to also re-encrypt and sign the message before sending it to the gaming machine as suggested by Nguyen.

32. In regard to claim 20, Nguyen in view of FIPS discloses the method of claim 16, but lacks disclosing the command comprising paying a bonus to a player at an electronic gaming machine.

33. In related prior art, Torango discloses a bonus system that generates bonus commands including paying a bonus (15:41-51). One skilled in the art would recognize the advantages of providing progressive games on a networked system to increase the size of the contributing player pool thereby offering larger potential payouts in order to attract players.

34. Therefore it would have been obvious to one skilled in the art at the time to combine the secure system of Nguyen with the progressive system of Torango to provide a secure progressive system thus providing large potential payouts to attract customers.

35. Claims 9-15 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Torango et al. (USPN 5885158) in view of Nguyen, Binh T. (US 20020071557 A1), Federal Information Processing Standards Publication 186 (FIPS) and Staring, Antonius A.M. (US 20010007127 A1).

36. In regard to claim 9, Torango discloses a progressive bonus system where the central server generates bonus commands (15:41-51). Torango further discloses the use of verification of hardware identification (16:1-13). Torango lacks disclosing performing a hashing function over at least a portion of a message that includes the bonus command to produce a message digest and then passing the message digest through a digital signature algorithm to produce a digitally signed bonus command; and transmitting the digitally signed bonus command from a transmitting node to an electronic gaming machine wherein the digitally signed bonus command from the transmitting mode is subjected to the hashing function to produce a message digest, the

message digest is passed through the digital signature algorithm to produce a digitally signed bonus command at the gaming machine, and the digitally signed bonus command at the gaming machine is compared to the digitally signed bonus command from the transmitting mode to determine if they match.

37. In related prior art, Nguyen discloses a system that is used to replace dedicated casino networks with secure communications over a general use network (par 15) where commands are digitally signed and transmitted to a gaming machine (par 62). Nguyen further discloses that some of the dedicated casino networks that may be replaced include network services for bonus game play, progressive game play and cashless ticketing (par 9). One skilled in the art would recognize the advantages of providing network security features to a networked progressive game system.

38. Therefore it would have been obvious to one skilled in the art at the time to combine the security system of Nguyen with the bonus system of Torango in order to provide a secure bonus system. The combination made lacks performing a hashing function over at least a portion of a message that includes the bonus command to produce a message digest and then passing the message digest through a digital signature algorithm to produce a digitally signed bonus command; and transmitting the digitally signed bonus command from a transmitting node to an electronic gaming machine wherein the digitally signed bonus command from the transmitting mode is subjected to the hashing function to produce a message digest, the message digest is passed through the digital signature algorithm to produce a digitally signed bonus command at the gaming machine, and the digitally signed bonus

command at the gaming machine is compared to the digitally signed bonus command from the transmitting mode to determine if they match.

39. In related prior art, FIPS discloses a digital signature standard that digitally signs a message by using a hash function in the signature generation process to obtain a condensed version of data, called a message digest (see Figure 1). The message digest is then input to the DSA to generate the digital signature. The digital signature is sent to the intended verifier along with the signed data (often called the message). The verifier of the message and signature verifies the signature by using the sender's public key. The same hash function must also be used in the verification process. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data. One skilled in the art would recognize the advantages of providing a secure way to authenticate the sender of a message in a network environment.

40. Therefore it would have been obvious to one skilled in the art at the time of the invention to have modified Torango in view of FIPS in order to have included the digital signature method of FIPS in order to provide a secure authentication process. The combination made lacks including a session key that is changeable and associated with an index so that a receiving node can determine the session key used.

41. In related prior art, Staring discloses that in encrypted systems it is useful to change session keys periodically (par 2) where the session keys are indexed so that a receiving node can determine the session key used (pars 12-14) to facilitate session key changes without the requirement of knowing what the decrypted data should look like (par 5). Staring further discloses that each message includes a session index

portion that is used to determine the session index of the receiving device in order to properly decrypt the message by testing the current and future session keys (par 40). Under this procedure, each message sent from the source includes the updated session key and each receiver knows the current session key that they are using. The receiving node thus is able to determine from the message what the updated session index and the corresponding key is from the key check data. One of ordinary skill in the art would recognize the advantages of changing session keys in order to increase security and providing a way for the receiving nodes to ensure they are using the proper key for decryption.

42. Therefore it would have been obvious to one of ordinary skill in the art to have modified Torango in view of Staring to have incorporated a session key index to facilitate frequent key changes for enhanced security while providing a way for the devices to determine the current session key to use. The combination does not explicitly disclose that the receiving node requests a new session key when the session index does not match the updated index.

43. However, one of ordinary skill in the art would have recognized that when applying the session index key check of Staring to a system where the receiving nodes did not have the ability to generate keys, it would be necessary for the clients to request a new key when the key check taught by Staring failed to match since such a system would have no more keys to try. Such a modification would have been readily understood by one of ordinary skill in the art, would have produced the expected result of getting the proper key to the device as would be needed to ensure operation of the

system, and would be in keeping with the teachings of Staring to implement. Accordingly, such a modification does not differentiate over the prior art.

44. In regard to claim 10, Torango discloses monitoring gaming machine play (5:32-44).

45. In regard to claim 11, Torango discloses determining if a machine is to receive a bonus (15:41-51).

46. In regard to claims 12, Torango discloses the central server generating a bonus command (13:56-14:11).

47. In regard to claim 13, Torango discloses that the slave server monitors communication and provide verification of prize wins (16:1-23). Torango lacks explicitly disclosing that the slave server generates the bonus command. However, it is well known in the art of network systems to have mirrored servers doing the same tasks to compensate for any network outages or problems. As such, it would have been an obvious modification to provide the slave server with the ability to handle bonus commands on its own in the event that the central server was unreachable.

48. In regard to claim 14, Torango discloses that the bonus commands are sent to the game machine through the cluster controller (15-52-59). Torango lacks explicitly stating that the messages are signed.

49. In related prior art, Nguyen discloses generating a signed command at the master server, sending it to the slave server, and the slave server decrypting the message and forwarding to the gaming machine (par 62). One skilled in the art would

recognize the advantages of providing secure messages for a financial transaction system on an unsecured network.

50. Therefore it would have been obvious to one skilled in the art at the time to combine the bonus system of Nguyen with the security system of Torango in order to provide a secure bonus server. The combination made lacks transmitting a second digitally signed bonus command to the electronic gaming machine.

51. However, Nguyen already discloses signing the messages on the way to the slave server from the gaming device (fig 4) and discloses that the slave server decrypts and then forwards the message to the gaming machine as stated above. It would be an obvious modification to also sign the message before sending it to the gaming machine as suggested by Nguyen as it would be mere duplication of steps.

52. In regard to claim 15, Torango in view of Nguyen, FIPS and Starling disclose the method of claim 9 above, but lacks wherein the method comprises transmitting an unsigned message after the generation of the bonus command and digitally signing the bonus command at a slave server. Rather the combination teaches signing the messages at the master server.

53. However, it would have been obvious to one skilled in the art that the operator of the game system would have the choice to use security measures on whatever portions of the system they chose as such a matter would have been mere design choice that fails to distinguish over the prior art.

54. In regard to claim 21, Torango discloses a bonus server system that pays bonuses to players as directed (15:41-51) and further discloses that the gaming

machines are verified by machine signatures and if invalid, the bonus is canceled (16:4-15). Torango lacks a digital signature; verifying the digital signature at a subservient device by subjecting the bonus message to a hashing function to produce a message digest, passing the message digest through a digital signature algorithm to produce a digital signature at the subservient device, and comparing the digital signature at the subservient device to the digital signal included with the command message to determine if there is a match.

55. In related prior art, Nguyen discloses a system that is used to replace dedicated casino networks with secure communications over a general use network (par 15) where commands are digitally signed and transmitted to a gaming machine (par 62). Nguyen further discloses that some of the dedicated casino networks that may be replaced include network services for bonus game play, progressive game play and cashless ticketing (par 9). One skilled in the art would recognize the advantages of providing network security features to a networked progressive game system.

56. Therefore it would have been obvious to one skilled in the art at the time to combine the security system of Nguyen with the bonus system of Torango in order to provide a secure bonus system. The combination made lacks subjecting the bonus message to a hashing function to produce a message digest, passing the message digest through a digital signature algorithm to produce a digital signature at the subservient device, and comparing the digital signature at the subservient device to the digital signal included with the command message to determine if there is a match.

57. In related prior art, FIPS discloses a digital signature standard that digitally signs a message by using a hash function in the signature generation process to obtain a condensed version of data, called a message digest (see Figure 1). The message digest is then input to the DSA to generate the digital signature. The digital signature is sent to the intended verifier along with the signed data (often called the message). The verifier of the message and signature verifies the signature by using the sender's public key. The same hash function must also be used in the verification process. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data. One skilled in the art would recognize the advantages of providing a secure way to authenticate the sender of a message in a network environment.

58. Therefore it would have been obvious to one skilled in the art at the time of the invention to have modified Torango in view of FIPS in order to have included the digital signature method of FIPS in order to provide a secure authentication process. The combination made lacks including a session key that is changeable and associated with an index so that a receiving node can determine the session key used.

59. In related prior art, Staring discloses that in encrypted systems it is useful to change session keys periodically (par 2) where the session keys are indexed so that a receiving node can determine the session key used (pars 12-14) to facilitate session key changes without the requirement of knowing what the decrypted data should look like (par 5). Staring further discloses that each message includes a session index portion that is used to determine the session index of the receiving device in order to properly decrypt the message by testing the current and future session keys (par 40).

Under this procedure, each message sent from the source includes the updated session key and each receiver knows the current session key that they are using. The receiving node thus is able to determine from the message what the updated session index and the corresponding key is from the key check data. One of ordinary skill in the art would recognize the advantages of changing session keys in order to increase security and providing a way for the receiving nodes to ensure they are using the proper key for decryption.

60. Therefore it would have been obvious to one of ordinary skill in the art to have modified Torango in view of Staring to have incorporated a session key index to facilitate frequent key changes for enhanced security while providing a way for the devices to determine the current session key to use. The combination does not explicitly disclose that the receiving node requests a new session key when the session index does not match the updated index.

61. However, one of ordinary skill in the art would have recognized that when applying the session index key check of Staring to a system where the receiving nodes did not have the ability to generate keys, it would be necessary for the clients to request a new key when the key check taught by Staring failed to match since such a system would have no more keys to try. Such a modification would have been readily understood by one of ordinary skill in the art, would have produced the expected result of getting the proper key to the device as would be needed to ensure operation of the system, and would be in keeping with the teachings of Staring to implement. Accordingly, such a modification does not differentiate over the prior art.

62. In regard to claim 22, Torango discloses manual intervention to resolve invalid payouts (16:15-21).

63. In regard to claim 23, Torango discloses that the bonus commands are sent to the game machine through the cluster controller (15-52-59). Torango lacks disclosing verifying the digital signature at the subservient device comprising generating a second command message, providing a digital signature to the second command message and transmitting the second command message with the digital signature.

64. In related prior art, Nguyen discloses generating a signed command at the master server, sending it to the slave server, and the slave server decrypting the message and forwarding to the gaming machine (par 62). One skilled in the art would recognize the advantages of providing secure messages for a financial transaction system on an unsecured network.

65. Therefore it would have been obvious to one skilled in the art at the time to combine the bonus system of Torango with the security system of Nguyen in order to provide a secure bonus server. The combination made lacks explicitly stating that the reply message is re-signed before sending it to the gaming machine.

66. However, Nguyen already discloses signing the messages on the way to the slave server from the gaming device (fig 4) and discloses that the slave server decrypts and then forwards the message to the gaming machine as stated above. It would be obvious to also re-encrypt and sign the message before sending it to the gaming machine as suggested by Nguyen.

Response to Arguments

67. Applicant's arguments filed 03/18/2009 have been fully considered but they are not persuasive. Applicant argues that Staring fails to disclose or suggest any use of session keys as recited in the amended claims. Examiner disagrees. In Staring, each message sent by the device includes the updated session key, which has a corresponding index. The receiving node uses the current session key on the message key check block to determine if the current session key and the corresponding index match the received or updated session key and its corresponding index. While Staring teaches that clients have the ability to generate keys and determine the next key, one of ordinary skill would have readily understood that in an instance whereby the client did not have the ability to generate a new key, the failure of the key check would necessitate a new key exchange with the host to obtain the current session key as otherwise the device would be nonfunctional. Thus Staring does provide a message with the updated session index so that the receiving nodes may determine if they are using the proper session key.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID DUFFY whose telephone number is (571) 272-1574. The examiner can normally be reached on M-F 0830-1700.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Peter Vo can be reached on (571) 272-4690. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. D./
Examiner, Art Unit 3714

/Corbett Coburn/
Primary Examiner
AU 3714